HP Docket No. 10003219-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:09/874,104
Conf. No.	:6048
Appellant	:Haines et al.
Filed	:06/04/2001
Title	:System And Method For Requesting Computer Resources
TC / Art Unit	:2444
Examiner	:Shingles, Kristie D.
Docket No.	:10003219-1
Customer No.	:022879

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

APPELLANTS' REPLY BRIEF

Sir:

This Reply Brief is presented in opposition to the Examiner's Answer mailed 03/16/2010. Appellants are appealing from the Final Rejection of claims 1, 3, 5-6, 8-11, 15, and 17-23.

I. ARGUMENT

The Examiner's Answer includes a "Response to Arguments" section at p. 12-16. In that section, the Examiner identifies Arguments A through D in the Appeal Brief, and then presents responses to these arguments. The present section of the Reply Brief follows the structure used in the Examiner's Answer, and presents counterarguments to the specific responses presented by the Examiner.

However, it should be noted that Appellants do not necessarily agree with the Examiner's characterization in the Examiner's Answer of the various arguments presented by Appellants in the Appeal Brief. Instead, Appellants rely on the arguments presented in the Appeal Brief, and the supplemental arguments presented in the Reply Brief.

Argument A

With regard to claims 1, 3, 5, and 21, and the claim limitation of "in response to receiving the second cookie, the web client transmitting the second cookie to the remote computer for storage", the Examiner conclusorily argues that the Combar reference teaches "a web browser-enabled client device receiving a URL response and a cookie for each HTTPS reply from the web/dispatch server and subsequently sending each received cookie to a separate cookie jar server for storage (col. 7, lines 27-41)" (Examiner's Answer, p. 12). The Examiner relied on this same portion of the Combar reference in the Final Rejection. In response, Appellants rely on their arguments presented at p. 9-12 of the Appeal Brief as to why the Examiner is incorrect in this conclusion.

The Examiner also argues that the Combar reference "states that the client holds the cookie and returns it to the remote cookie jar server (col. 7 lines 32-34)" (Examiner's Answer, p. 12). However, the Examiner fails to fully construe the limitation. As Appellants argued at p. 11 of the Appeal Brief, a complete construction of the limitation requires that the web client transmit the second cookie to the remote computer for storage in response to receiving the second cookie. Conversely, what the Combar reference teaches the client does, in response to receiving the second cookie, is to hold it. The cookie is transmitted only if the client makes a subsequent HTTPS request; if no such request is made, the cookie is not transmitted. Such a conditional transmission cannot be construed as being "in response to" the receipt of the cookie by the client.

Thus the Sears and Combar references in combination fail to teach or suggest at least these limitations recited in the claims.

With regard to an articulated reason with some rational underpinning as to why the teachings of the Sears reference should be modified according to the teachings of the Combar

reference, the Examiner argues that "the rationale that storing cookies a separate/remote cookie jar server adds 'an additional level of security' to the system (Combar et al, col. 6 lines 40-41). This modification is not unreasonable nor is the motivation to combine impractical based on the functionality of the inventions described in Combar et al and Sears, Jr. et al." (Examiner's Answer, p.13). Appellants disagree. There is no need to use the teachings of the Combar references in order to allow the Sears reference to store cookies in a separate/remote cookie jar server. The Sears reference already teaches this feature. As can be understood from Fig. 3, the Sears reference discloses a separate cookie server 310; separate from client 320, weather web sites 330,370, and news web site 340. Thus the Sears reference, without requiring any of the teachings of the Combar reference, already provides the additional level of security that a separate cookie server provides. Thus the reason articulated by the Examiner for combining the references does not have the required rational underpinning to serve as motivation to modify or combine the references. Instead, the Combar reference is impermissibly used in hindsight by the Examiner, utilizing Appellants' claims as a template in an attempt to somehow cobble together pieces of the different references.

Argument B

With regard to the rejection of claims 6, 8-11, and 22, the claim limitation of "means for receiving at the computing device, from a first web client, a first cookie that is valid for a first range of URL's, the first cookie provided to the first web client by a web server" recites three actors: the computing device (i.e. a cookie store), the first web client, and the web server. With regard to this limitation, the Examiner argues that the Dutta reference discloses that "the server-side storage receives a cookie from a client, with the cookie being provided to the client by a content producer web server to determine which pages are accessible to the client (col. 4 lines 50-59, col 6 lines 6-10 and 24-27)" (Examiner's Answer, p. 13-14). Thus the Examiner's position is that the Dutta reference also discloses three actors: the server-side storage, the client, and the content producer web server.

Appellants disagree. The Dutta reference discloses that only two actors are involved in the cookie transfers: the web client 103 and the content producer web site 101. The user

(i.e. client 103) iteratively interacts with the content producer web site 101 (i.e. http://www.producer.com) to step through a series of hierarchical links to ultimately get to the desired web page (i.e. jaws.html) (see Dutta, col. 5, ln. 23 – col. 6, ln. 52). During these iterative interactions, a cookie is passed between the web client 103 and the content producer web site 101; there is no third actor in these transactions. The only third actor disclosed in the Dutta reference at all is the content aggregator web server 102 (Fig. 1). However, there is no disclosure that the web client 103 ever provides to the content aggregator web server 102 any cookie provided to the web client 103 by the content producer web site 101. With regard to the content aggregator web server 102, the Dutta reference discloses only that the web client 103 "first connects to the content aggregator 102 in communication 1 and receives a response in communication 2. The response is a pointer to the content producer which the Web client 103 goes to via communication 3" (Dutta, col. 4, ln. 2-6). From that point on, all communications are between the web client 103 and the content producer web site 101.

Thus the Dutta and Quatrano references in combination fail to teach or suggest at least these limitations recited in the claims.

With regard to an articulated reason with some rational underpinning as to why the teachings of the Dutta and Quatrano references should be combined, the Examiner argues that the motivation "was to achieve the claim limitations" (Examiner's Answer, p.14). Appellants do not agree that this articulated reason has sufficient rational underpinning, because the combination would render the Dutta reference inoperative. The Dutta reference is directed to restricting a client from deep hyperlinking to a content producer's web site, by instead rerouting such request to the content producer's home page and requiring the client to view items such as one or more advertisements on certain pages before obtaining the desired content (Dutta, Abstract; col. 3, ln. 18-21). If shared access were provided to the web site for multiple users, then once a single one of the users viewed the advertisements, all the other shared users would also be able to obtain the content via direct deep hyperlinking, using the shared cookie, without having to view the advertisements desired by the content producer. This renders the Dutta reference inoperative for its intended purpose of restricting deep hyperlinking. Thus not does the articulated reason lack the required rational underpinning,

but the Dutta reference also teaches away from the combination made by the Examiner because to do so would render it inoperative.

Argument C

With regard to claims 15, 17, and 23, and claim limitations in which first/second web clients are operable to receive a first/second cookie from a web server and automatically transmit the first/second cookie to a remote computer, the Examiner admits that the Quatrano reference "does not teach the participant sending the cookie to a remote server for storage". However, the Examiner argues that the Combar reference teaches "a user's web-enabled client device receiving a URL request input from the user, and the user's web-enabled client device receiving the resource and a cookie for each HTTPS request from the web/dispatch server, and subsequently sending each cookie to a separate cookie jar for storage (Figure 2, col. 7 lines 27-41)", "that the client holds the cookie and returns it to the cookie jar server (col. 7 lines 32-34)", and "that the web/dispatch server and the cookie jar server are separate devices" (Examiner's Answer, p.15-16).

Appellants disagree that the combined teachings of the Quatrano and Combar references teach or suggest these limitations. First, the limitations require that the clients transmit the first/second cookie to a remote computer. It is unclear which element of which reference the Examiner considers to correspond to the recited remote computer.

To the extent that the Examiner considers application server 50 of the Quatrano reference to be the remote computer, the Appeal Brief, p. 20-21, presents several arguments as to why the combined references fail to teach or suggest these limitations.

To the extent that the Examiner considers cookie jar server 28 of the Combar reference to be the remote computer, the Combar reference discloses that the client (customer browser 20) does not communicate with the cookie jar server 28, and thus cannot return the cookie to the cookie jar server 28. The Combar reference discloses instead that "Customer Browser 20, is browser enabled and includes client applications responsible for presentation and front-end services. Its functions include providing a user interface to various MCI services and supporting communications with MCI's Intranet web server cluster 24" (col. 5,

ln. 24-28; emphasis added). As can be appreciated from Fig. 2, client browser 20 has no connection to cookie jar server 28. Instead, "after one of the DMZ Web servers 24 decrypts and verifies the user session, it forwards the message through a firewall 25b over a TCP/IP connection 23 to the dispatch server 26 on a new TCP socket while the original socket 22 from the browser is blocking, waiting for a response" (col. 7, ln. 42-47; emphasis added). Thus it is web server 24, not client browser 20, that communicates with dispatch server 26. While there is no explicit statement in the Combar reference that it is web server 24 that communicates with cookie jar server 28, cookie jar server 28 is illustrated in Fig. 2 as being at the same position in the data flow as dispatch server 26, and thus the communication process with cookie jar server 28 must necessarily be the same as with dispatch server 26.

In addition, the Examiner is incorrect in arguing that the client holds the cookie and returns it to the cookie jar server. The Combar reference discloses instead that "the client holds the cookie and returns it to the server as part of each subsequent HTTPS request" (col. 7, ln. 32-34; emphasis added). The reference does not explicitly identify which server – web server 24, dispatch server 26, cookie jar server 28, or any of the other various servers illustrated in Fig. 2 – the client returns the cookie to. Considering the entirety of the teachings of Fig. 2, the only operable interpretation is that the client browser 20, using the above-described communication process, returns the cookie to web server 24, which in turn decrypts, verifies, and forwards the cookie through firewall 25b over TCP/IP connection 23 to cookie server 28 on a new TCP socket while the original socket 22 from the browser is blocking, waiting for a response.

Second, the claim limitations require that the first/second web clients automatically transmit the first/second cookie to a remote computer after receiving it. The Quatrano and Combar references, individually or in combination, do not teach or suggest any such automatic transmission of a cookie from a client to a cookie store. As argued in the Appeal Brief, p. 20-21, the Quatrano reference discloses, at most, that the cookie may be transmitted by the web client 10,20 to the web server 30 in response to a user of web client 10,20 manually interacting with the shared session at a subsequent time. And for similar reasons as discussed heretofore with reference to Argument A of this Reply Brief, the Combar reference

teaches that the client holds the cookie after receiving it; no automatic transmission is performed. The cookie is transmitted only if the client makes a subsequent HTTPS request; if no such request is made, the cookie is not transmitted.

Thus the Quatrano and Combar references in combination fail to teach or suggest at least these limitations recited in the claims.

Argument D

The Examiner argues that the rejection of claims 18-20 is maintained since the rejection of base claim 15 is proper. For the reasons argued above, Appellants believe that the rejection of base claim 15 is improper and thus the rejection of claims 18-20 is also improper.

II. CONCLUSION

Appellants contend that claims 1, 3, 5-6, 8-11, 15, and 17-23 were improperly rejected because the applied references, alone or in combination, do not teach or suggest all of Appellants' claim limitations, there is no articulated reason with some rational underpinning to modify or combine reference teachings, impermissible hindsight is used to combine or modify the references, one or more of the references teach away from the combination, and/or there is no reasonable expectation of success in combining the references.

Each of these reasons alone distinguishes Appellants' claims from the cited references and makes Appellants' claims non-obvious in light of the cited references.

Overruling of the Examiner's rejections of claims 1, 3, 5-6, 8-11, 15, and 17-23 is respectfully requested.

HP Docket No. 10003219-1

AUTHORIZATION TO PAY AND PETITION

FOR THE ACCEPTANCE OF ANY NECESSARY FEES

If any charges or fees must be paid in connection with the foregoing communication (including but not limited to the payment of an extension fee or issue fees), or if any overpayment is to be refunded in connection with the above-identified application, any such charges or fees, or any such overpayment, may be respectively paid out of, or into, the Deposit Account No. 08-2025 of Hewlett-Packard Company. If any such payment also requires Petition or Extension Request, please construe this authorization to pay as the necessary Petition or Request which is required to accompany the payment.

Respectfully submitted,

/Robert C. Sismilich/

Robert C. Sismilich
Reg. No. 41,314
Attorney for Appellant(s)
Telephone: (941) 677-6015

Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400